Joint Task Force
National Capital Region Medical
DIRECTIVE

SUBJECT: Information Assurance (IA) Training, Certification, and Workforce Management

References: See Enclosure 1

1. <u>PURPOSE</u>. This Directive, in accordance with the authority in References (a) through (d):

   a. Establishes policy and assigns responsibilities, according to DoD Directive 8500.01E, DoD Instruction 8500.02, DoD Directive O-8530.1, DoD 8570.01 (References (e) through (h)) for Joint Task Force National Capital Region Medical (JTF CapMed) IA training, certification, and workforce management.

   b. Authorizes the publication of issuances implementing the policy in this Directive.

2. <u>APPLICABILITY</u>. This Directive applies to:

   a. JTF CapMed and all Joint Medical Treatment Facilities and Centers in the National Capital Region (i.e., Fort Belvoir Community Hospital, Walter Reed National Military Medical Center, and the Joint Pathology Center).

   b. Contracts for personnel providing IA functional services for JTF CapMed information systems (IS) via appropriate Defense Federal Acquisition Regulation Supplement (DFARS) clauses.

3. <u>DEFINITIONS</u>. See Glossary

4. <u>POLICY</u>. It is JTF CapMed policy that:

   a. All authorized users of JTF CapMed IS shall receive initial IA awareness orientation as a condition of access and thereafter must complete annual IA refresher awareness.

b. Privileged users and IA managers shall be fully qualified per Reference (g), trained, and certified to DoD baseline requirements to perform their IA duties.

c. Personnel performing IA privileged user or management functions, regardless of job series or military specialty, shall be appropriately identified in the JTF CapMed Component personnel databases.

d. All IA personnel shall be identified, tracked, and managed so that IA positions are staffed with personnel trained and certified by category, level, and function.

e. All positions involved in the performance of IA functions shall be identified in appropriate manpower databases by category and level.

f. The status of the JTF CapMed Joint MTF and Center IA certification and training shall be monitored and reported as an element of mission readiness and as a management review item per Reference (g).

g. IA Workforce Structure (Enclosure 3) shall focus on the development, operation, management, and enforcement of security capabilities for systems and networks.

h. IA Workforce Categories and Levels (Enclosure 4) outlines overall categories within the IA workforce.

5. RESPONSIBILITIES. See Enclosure 2

6. RELEASABILITY. UNLIMITED. This Directive is approved for public release and is available on the Internet from the JTF CapMed Web Site at: www.capmed.mil.

7. EFFECTIVE DATE. This Directive is effective immediately.

STEPHEN L. JONES
Major General, U.S. Army
Deputy Commander

Enclosures
1. References
2. Responsibilities
3. JTF CapMed IA Workforce Structure
4. JTF CapMed IA Workforce Categories and Levels

2

ENCLOSURE 1

REFERENCES

(a) Deputy Secretary of Defense Memorandum, "Establishing Authority for Joint Task Force – National Capital Region/Medical (JTF CapMed) and JTF CapMed Transition Team (Unclassified)," September 12, 2007

(b) Deputy Secretary of Defense Action Memorandum, "Civilian and Military Personnel Management Structures for the Joint Task Force National Capital Region – Medical," January 15, 2009

(c) Comprehensive Master Plan for the National Capital Region Medical, April 23, 2010

(d) Supplement to the Comprehensive Master Plan for the National Capital Region Medical, August 31, 2010

(e) DoD Directive 8500.01E, "Information Assurance," October 24, 2002

(f) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

(g) DoD Directive O-8530.1, "Computer Network Defense," January 8, 2001

(h) DoD 8570.01 "Information Assurance Workplace Improvement Program"

(i) Office of Personnel Management Job Family Position Classification Standard for Administrative Work in the Information Technology Group, GS-2200; Information Technology Management GS-2210, May 2001, revised August 2003

(j) MHS-TMA Standard Operating Procedure, "Military Health System/TRICARE Management Activity"

ENCLOSURE 2

RESPONSIBILITIES

1. <u>JTF J-6 CIO</u>. The JTF J-6 CIO shall:

a. Develop and promulgate additional guidance relating to IA training, certification, and workforce management requirements.

b. Coordinate the integration of IA initiatives with other workforce development and sustainment requirements.

c. Establish metrics to monitor and validate compliance with this Directive as an element of mission readiness.

d. Provide recommended changes to the DFARS to reflect requirements of this Directive relating to contracts and contractors.

e. Ensure that all DoD civilian positions and personnel, regardless of Office of Personnel and Management (OPM) series or job title, with IA functions shall use "INFOSEC" as the Position Specialty Code in the Defense Civilian Personnel Data System.

2. <u>JTF J-6 CHIEF OF IA</u>. The JTF J-6 Chief of IA shall:

a. Provide web-based access to current IA policies, techniques, requirements, and knowledge resources to support life-cycle enhancement of IA workforce functional competencies.

b. Provide baseline training and awareness materials, content, and products on IA policies, concepts, procedures, tools, techniques, and systems for the JTF CapMed to integrate into their IA training and awareness programs.

c. Enforce compliance with the DoD issuances, ensuring the IA workforce training and certification program.

d. Establish, resource, and implement IA training and certification programs for all JTF CapMed personnel in accordance with this Directive and References (e), (f), and (g). These programs shall train, educate, certify, and professionalize personnel commensurate with their responsibilities to develop, use, operate, administer, maintain, defend, and retire DoD IS.

e. Ensure promotion of and compliance with baseline IA training, certification, and tracking program for the Designated Approving Authority.

3. <u>JOINT MTF COMMANDERS AND CENTER DIRECTORS</u>. Joint MTF Commanders and Center Directors shall:

    a. Monitor compliance with initial IA awareness orientation and annual IA refresher awareness to authorized users.

    b. Identify, document, and track IA personnel certifications and certification status in component personnel databases.

    c. Identify military IA billets in manpower databases based on operational mission support and force structure requirements.

    d. Ensure the use of the existing abbreviation for Security, "INFOSEC," established in the OPM General Schedule-2210 series (Reference (i)) to support DoD-wide civilian IA workforce identification and management requirements.

    e. Require contracts that include the acquisition of JTF CapMed IS IA services to specify certification requirements. Ensure that contractor personnel performing IA functions have their IA certification category and level documented in the Defense Eligibility Enrollment Reporting System.

    f. Identify, document, track, and report to the DoD CIO the certifications and certification status of all military, civilians, and contractors performing privileged user or IA manager functions in accordance with Reference (h).

    g. Provide appropriate IA training for personnel required to enforce DoD IA requirements per this Directive and the references listed herein.

    h. Include IA awareness training and education, as appropriate, in professional military education at all levels.

ENCLOSURE 2

ENCLOSURE 3

JTF CAPMED IA WORKFORCE STRUCTURE

1. Personnel performing IA functions establish IA policies and implement security measures and procedures for the Department of Defense and affiliated information systems and networks.

2. IA measures protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for their restoration by incorporating protection, detection, and reaction capabilities.

3. IA duties may be performed as primary or additional/embedded duties, by a DoD employee (civilian, local nationals, including military) or by a support contractor.

4. As a condition of privileged access to any information system, personnel performing IA functions described in this Directive must satisfy both preparatory and sustaining DoD IA training and certification requirements.

5. The certification requirements of Reference (h) apply to DoD civilian employees, military personnel, local nationals, and support contractors performing IA functions.

6. Personnel performing IA duties addressed by this policy include the following IA oversight responsibilities:

   a. Work closely with data owners, information system owners, and users to ensure secure use and operation of IS and networks.

   b. Ensure rigorous application of IA policies, principles, and practices in the delivery of all information technology (IT) services.

   c. Maintain system audit functions and periodically review audit information for detection of system abuses.

   d. Identify IA requirements as part of the IT acquisition development process and ensure MHS standard contract language for IA is included in all IT acquisitions contract and statement of work.

   e. Ensure the MTFs and Centers IT support functions assess and implement identified corrections (e.g., system patches and fixes) associated with technical vulnerabilities as part of the IA Vulnerability Management program.

f. Ensure the MTFs and Centers maintain configuration control of hardware, systems, and application software.

g. Ensure the MTFs and Centers identify and properly react to security anomalies or integrity loopholes such as system weaknesses or vulnerabilities.

h. Ensure the MTFs and Centers install and administer user identification or authentication mechanisms.

ENCLOSURE 4

JTF CAPMED IA WORKFORCE CATEGORIES AND LEVELS

1. Reference (h) identifies two overall categories within the IA workforce: Technical and Management. These categories are subdivided into three levels each based on functional skill requirements and system environment focus (see Chapters 3, 4, and 5 of Reference (h)).

2. The levels and functions provide the basis to determine all IA technical and management staffing requirements. They also provide a framework for the identification of IA technical and management positions and qualified personnel (or those who can become qualified) across the Department of Defense.

3. Each Department of Defense position responsible for IA functional requirement(s) must be correlated with a category and level. Assigning position levels based on functions across the Department of Defense establishes a common framework for identifying the IA workforce.

4. A position may include functional requirements spanning multiple levels. In these cases, the level, and related certification requirements, will be those of the highest level functions. Individuals performing both Information Assurance Technician (IAT) and Information Assurance Manager (IAM) category functions must hold certifications appropriate to the functions performed in each category.

5. IA workforce categories and levels do not necessarily correlate to civilian grades, military ranks, or any specific occupational classification standard.

6. Technical category training requirements are summarized in Table 1 of Reference (h).

7. JTF CapMed IA Personnel will comply with the Military Health System/TRICARE Management Activity (MHS-TMA) Standard Operating Procedure (SOP) (Reference (j)).

    a. The MHS/TMA IA Program Office requires that all personnel working on the MHS/TMA certification and accreditation (C&A) project be fully qualified, trained, and certified to DoD baseline requirements to perform their IA duties. As per the MHS/TMA IA Performance Work Statement, key personnel will be required to obtain/maintain their security certification (e.g., Certified Information Systems Security Professional) at the start while all others obtain their certification within six months of hire.

ENCLOSURE 4

b. Additionally, per the MHS/TMA IA Program Office, all personnel are to be trained on the MHS/TMA IA C&A process, SOP, and the IA Lab Applications.

8. JTF CapMed IA Workforce Certification Levels:

   a. JTF Certifying Authority (CA) is designated IAM Level III.

   b. JTF CA Team is designated IAM and IAT Level III.

   c. The IA teams for organizations assigned to JTF CapMed Joint MTFs and Centers are designated IAM and IAT Level II.

ENCLOSURE 4